FORUM

KI in der Beschaffung

Sehr geehrte*r Leser*in,

Künstliche Intelligenz stellt den Einkauf vor neue Herausforderungen von der richtigen Einordnung der Systeme bis hin zur sicheren Integration in bestehende Prozesse. Parallel nehmen regulatorische Anforderungen durch EU AI Act, Datenschutz und Compliance spürbar zu.

Dieses Whitepaper bietet Ihnen eine fundierte Orientierung, wie Sie KI-Lösungen verantwortungsvoll beschaffen, Risiken gezielt steuern und vertraglich absichern. Sie gewinnen Klarheit über zentrale Fragestellungen und erhalten praxisnahe Impulse für eine sichere und zukunftsfähige Beschaffung.

Dieses Whitepaper wurde mithilfe des KI-Tools DeepResearch von OpenAI erstellt. Es beleuchtet aktuelle Entwicklungen rund um KI in der Beschaffung, insbesondere im Kontext von EU AI Act, Vergaberecht und Compliance-Anforderungen. Neben regulatorischen Vorgaben werden zentrale Trends wie Digitalisierung, Risikosteuerung und der Einsatz lernender Systeme praxisnah eingeordnet.

Dieses Whitepaper orientiert sich am Anwendungsfall der regulierten Beschaffung in Deutschland und zeigt zugleich auf, wie sich die dargestellten Ansätze auf private Unternehmen und öffentliche Auftraggeber übertragen lassen. Da weder eine spezifische Branche noch ein bestimmtes Sektorrecht im Fokus stehen, werden sowohl die Perspektive der öffentlichen Vergabe als auch der privaten Beschaffung berücksichtigt.

Sektorspezifische Anforderungen etwa aus dem Bereich der Medizinprodukte, der Finanzaufsicht oder KRITIS werden dort einbezogen, wo sie für die Ausgestaltung von Beschaffungsprozessen unmittelbar relevant sind. Auf diese Weise entsteht ein praxisnaher, übertragbarer Rahmen für den Einsatz von KI in der Beschaffung.

- KI ist beschaffungsrechtlich und vertraglich kein gewöhnlicher Softwareeinkauf. Für Hochrisiko-KI verlangt die KI-Verordnung einen fortlaufenden Lebenszyklusansatz mit Risikomanagement, Tests, technischer Dokumentation, Logging, Transparenz gegenüber Betreibern, menschlicher Aufsicht, Genauigkeit/Robustheit/Cybersecurity sowie Post-Market-Monitoring. Für lernende oder nach Inbetriebnahme veränderte Systeme ist deshalb ein einmaliger Abnahmepunkt regelmäßig unzureichend.

- Beschaffung muss mit einer vorgelagerten Einordnung beginnen: Fällt die Lösung überhaupt unter die KI-Verordnung, handelt es sich um verbotene Praktiken, nur um Transparenzpflichten, um GPAI-Modelle oder um Hochrisiko-KI? Parallel gilt seit Februar 2025 bereits die Pflicht zur KI-Kompetenz; bloßes Bereitstellen einer Bedienungsanleitung genügt dafür regelmäßig nicht.

- Verträge müssen die Rollen in der Wertschöpfungskette sauber zuweisen und Beweis-, Kontroll- und Eingriffsrechte absichern. Zentral sind Dokumentationszugang, Audit- und Testrechte, Update- und Change-Control, Ausschluss des Trainings mit Kund*innendaten bzw. Eingaben/Ausgaben, Incident-Meldung, Unterstützung bei DSFA/GRFA, Exit- und Portabilitätsregeln sowie klare Haftungs- und Freistellungsmechanismen.

- Datenschutzrecht läuft neben der KI-Verordnung weiter und wird durch sie nicht ersetzt. Nach den Leitlinien der Datenschutzkonferenz und der Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wird für viele KI-Einsätze eine Datenschutz-Folgenabschätzung regelmäßig erforderlich sein; bei bestimmten Hochrisiko-Einsätzen öffentlicher Stellen kommt ergänzend eine Grundrechte-Folgenabschätzung hinzu.

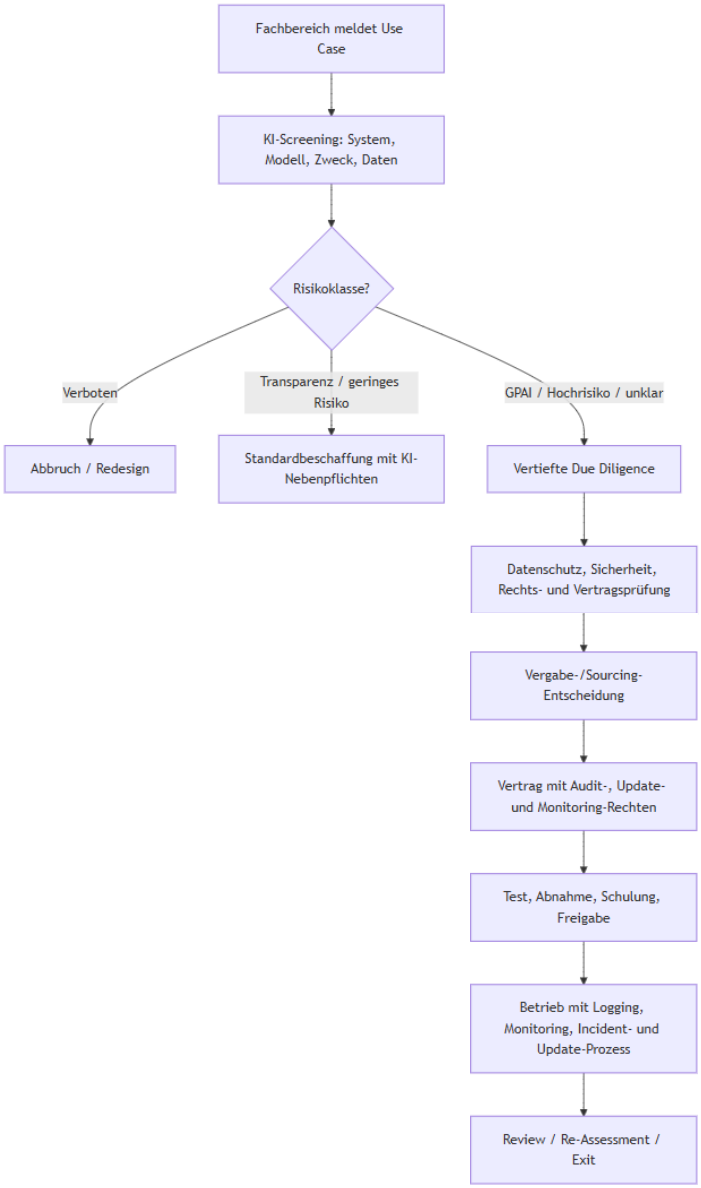
- Die nationale Umsetzung der KI-Verordnung ist in Deutschland im Aufbau. Nach der Beratung im Deutscher Bundestag soll die Bundesnetzagentur eine zentrale Rolle als Marktüberwachungs- und Koordinierungsstelle übernehmen; gleichzeitig baut sie bereits einen KI-Service-Desk, einen Compliance-Kompass und ein KI-Reallabor auf. Unternehmen sollten deshalb nicht auf das endgültige nationale Begleitgesetz warten, sondern ihre Beschaffungs- und Vertragsmuster jetzt harmonisieren.

- Der „Digitale Omnibus“ verändert die Planungslage. Die Europäische Kommission hat Ende 2025 gezielte Vereinfachungen für den KI-, Cyber- und Datenrahmen vorgeschlagen; der Rat der Europäischen Union hat im März 2026 seine Verhandlungsposition beschlossen, und das Europäisches Parlament war im Frühjahr 2026 im Mandatsaufbau. Für Beschaffung und Verträge bedeutet das: mit Re-Opener-Klauseln, Update-Governance und Terminpuffern arbeiten, statt starre 2026/2027-Annahmen in Stein zu meißeln.

Ausgangslage und Annahmen

Beschaffung von KI unterscheidet sich von klassischer IT-Beschaffung vor allem aus drei Gründen. Erstens hängt die regulatorische Einordnung stärker am *intendierten Zweck* als am Marketing des Anbieters. Zweitens erzeugen dynamische oder feinjustierte Systeme Risiken, die erst im Betrieb sichtbar werden können; der AI-Act adressiert das ausdrücklich über Risikomanagement, Logging, Post-Market-Monitoring und Incident-Meldung. Drittens können Downstream-Änderungen – etwa Rebranding, substanzielle Anpassungen oder neue Zweckbestimmungen – dazu führen, dass ein einkaufendes bzw. implementierendes Unternehmen regulatorisch in provider-nahe Verantwortung rutscht.

Für die Beschaffungspraxis folgt daraus: KI darf nicht als „Innovations-Sonderfall neben dem Regelbetrieb“ organisiert werden. Der sachgerechte Ansatz ist ein gestufter Standardprozess innerhalb von Source-to-Procure bzw. Purchase-to-Pay, ergänzt um KI-spezifische Gates für Klassifikation, Risiko, Datenschutz, Sicherheit, Evidenzprüfung und Betriebsfreigabe. Genau dieses frühe, in den Beschaffungszyklus integrierte Vorgehen empfehlen sowohl die Aufsichtspraxis im Datenschutz als auch die deutschen Umsetzungsinstrumente zur KI-Verordnung.



Der Entscheidungsfluss oberhalb verdichtet die Anforderungen der KI-Verordnung, der Datenschutzaufsicht und der deutschen Umsetzungs- und Orientierungshilfen in ein operatives Beschaffungsmodell.

Rechtsrahmen, Pflicht-Compliance und nationale Umsetzung

Der Grundtext der KI-Verordnung ist seit August 2024 in Kraft. Nach Artikel 113 gelten die Verbote, Definitionen und Regeln zur KI-Kompetenz seit Februar 2025; Governance-Regeln und GPAI-Pflichten gelten seit August 2025. Der Basistext sieht die generelle Anwendung ab 2. August 2026 vor; zugleich wird in aktuellen offiziellen FAQs und Umsetzungsseiten bereits mit einem Roll-out bis 2. August 2027 gearbeitet, weil die Hochrisiko-Regeln politisch mit Standardisierung und Unterstützungsinstrumenten verzahnt werden. Für GPAI-Modelle gilt zudem: Pflichten greifen seit August 2025; Modelle, die vor diesem Datum auf dem Markt waren, müssen bis August 2027 nachgezogen werden.

Die Kommission hat den Digitalen Omnibus als Vereinfachungspaket für KI, Cybersecurity und Daten vorgestellt. Nach offizieller Darstellung soll das Paket unter anderem gezielte Änderungen an der KI-Verordnung, größere Spielräume für Real-World-Testing und zentralisierte Aufsichtselemente bringen; die Hochrisiko-Regeln sollen erst dann greifen müssen, wenn notwendige Support-Tools und Standards verfügbar sind. Stand April 2026 befindet sich dieses Paket jedoch noch im Gesetzgebungsverfahren. Für den Einkauf heißt das nüchtern: Man sollte weder auf Vollzug warten noch nur mit dem ursprünglichen Stichtag planen, sondern vertraglich mit regulatorischen Änderungsmechanismen arbeiten.

Für Deutschland ist die Lage zweigeteilt. Die Verordnung gilt als EU-Rechtsakt unmittelbar, zugleich müssen Zuständigkeiten, Marktüberwachung, Notifizierung und Bußgeld-/Verfahrensregeln national ausgestaltet werden. Nach dem Regierungsentwurf des KI-Marktüberwachungs- und Innovationsförderungs-Gesetzes soll die Bundesnetzagentur zentrale Marktüberwachungsbehörde werden, ein Koordinierungs- und Kompetenzzentrum sowie eine Beschwerdestelle aufbauen und mindestens ein KI-Reallabor betreiben. Parallel betreibt die Behörde bereits einen KI-Service-Desk, einen KI-Compliance-Kompass und Hilfen zur KI-Kompetenz.

Pflicht-Compliance für KI ist deshalb kein Einzelgesetz, sondern ein Bündel paralleler Regime. Im Kern sind mindestens zu prüfen: KI-Verordnung, Datenschutzrecht, Informationssicherheit/Cybersecurity, Urheber- und Geheimnisschutz, Vertrags- und Haftungsrecht, arbeits- oder mitbestimmungsrechtliche Implikationen sowie – bei öffentlichen Auftraggebern – Vergaberecht. Bei Hochrisiko-KI treten insbesondere Dokumentation, Logging, Transparenz, menschliche Aufsicht, Qualitätssicherung, Registrierung und Post-Market-Monitoring in den Vordergrund; bei GPAI-Modellen kommen insbesondere Transparenz-, Copyright- und Dokumentationspflichten hinzu.

KI im Regelbetrieb beschaffen

Der belastbare Standardprozess beginnt mit einer fachlichen und rechtlichen *Use-Case-Klassifikation*. Dabei werden nicht nur Produktname und Anbieter, sondern insbesondere Zweck, Zielgruppe, Datenarten, Eingriffsintensität, Autonomiegrad, Betroffenenkreis und vorgesehene Automatisierung bewertet. Diese Logik folgt unmittelbar aus der risikobasierten Architektur der KI-Verordnung, aus den Auslegungshilfen zur KI-Definition und aus der Anforderung, KI-Kompetenz rollen- und kontextbezogen aufzubauen.

Im Regelbetrieb sollte die Beschaffung deshalb in sechs Prüffelder gegliedert werden: Rollenklärung in der Wertschöpfungskette, regulatorische Klassifikation, Verwendungs- und Datenarchitektur, Evidenz und

Dokumentation des Anbieters, Betriebs- und Update-Modell sowie Exit-/Fallback-Fähigkeit. Besonders wichtig ist die Rollenklärung: Wer heute nur Betreiber ist, kann morgen bei substantieller Anpassung, Rebranding oder eigenem Fine-Tuning in provider-nahe Pflichten hineinwachsen. Bei GPAI-Konstellationen ist außerdem zu prüfen, ob der Downstream-Akteur durch erhebliche Modifikation selbst zum Anbieter eines GPAI-Modells wird.

Vergleich von Beschaffungsansätzen

Standard-SaaS mit KI-Funktion

Typischer Einsatz: Klare Prozesse mit geringem Risiko
Vorgehen: Standardbeschaffung mit ergänzender KI-Prüfung
Worauf es ankommt: Datennutzung, Update-Transparenz, Exit-Regeln
Typischer Fehler: KI-Anteil wird vertraglich nicht sauber abgegrenzt

Konfigurierbare KI-Plattform mit Pilot

Typischer Einsatz: Anpassungsbedürftige Fachprozesse
Vorgehen: Pilotphase mit klar definierten Go-/No-Go-Gates
Worauf es ankommt: KPIs, Abnahme je Phase, Human Oversight
Typischer Fehler: Pilot wird zum Dauerzustand ohne klare Entscheidung

Verhandlungs-/Dialogverfahren

Typischer Einsatz: Hohe Komplexität, unklare Zielarchitektur
Vorgehen: Iterativer Austausch mit dem Markt
Worauf es ankommt: Dokumentation, Bewertungslogik, Transparenz
Typischer Fehler: Anforderungen werden nicht ausreichend konkretisiert

Die oben genannten Inhalte verdichten die in der öffentlichen Beschaffung verfügbaren Instrumente insbesondere Marktkonsultation, Verhandlungsverfahren, wettbewerblichen Dialog und Innovationspartnerschaft auf KI-typische Beschaffungssituationen; für private Beschaffung lassen sich dieselben Strukturentscheidungen sinngemäß übertragen. Das Sachargument für KI ist fast immer dasselbe: Wo Lösungsraum, Datenlage, Trainings- oder Update-Modell nicht vollständig standardisiert sind, ist ein reines Lowest-Price- oder Katalogmodell regelmäßig zu schwach.

Praktische Checkliste vor Ausschreibung oder Beauftragung

- Ist dokumentiert, *welches* Problem gelöst werden soll und warum dafür überhaupt KI erforderlich ist?
- Ist das System nach KI-Verordnung klassifiziert: verboten, transparent, GPAI, Hochrisiko, unklar?
- Ist bestimmt, ob das Unternehmen bloß Betreiber ist oder durch Anpassung/Branding/Fine-Tuning provider-nahe Pflichten übernimmt?
- Sind Datenquellen, Datenarten, personenbezogene Daten, besondere Kategorien und Geheimhaltungsstufen kartiert?
- Liegt eine erste Datenschutz-Vorabprüfung vor; ist eine DSFA wahrscheinlich?
- Gibt es Mindestanforderungen an Logging, Human Oversight, Incident-Prozess, Updates und Exit?
- Wurden Fachbereich, Einkauf, Recht/Compliance, Informationssicherheit und Datenschutz frühzeitig eingebunden?
- Ist die KI-Kompetenz der beteiligten Rollen geplant, dokumentiert und budgetiert?

Diese Checkliste leitet sich aus der KI-Kompetenzpflicht, der DSFA-/GRFA-Logik, der Rollenklärung entlang der KI-Wertschöpfungskette und den Hochrisiko-Anforderungen ab.

Risikosteuerung, Mindestanforderungen und lernende Systeme

Lernende und dynamische Systeme verschieben das Beschaffungsrisiko von der einmaligen Lieferprüfung in die Betriebsphase. Official FAQs zum AI Act stellen klar, dass Weiterentwicklungen von Hochrisiko-Systemen innerhalb des Risikomanagementrahmens antizipiert werden müssen; substanzielle Änderungen können eine neue Konformitätsbewertung auslösen. Das gilt praktisch besonders bei Modell-Updates, Änderung der Systemarchitektur, Wechsel der Datengrundlage, geänderten Schwellenwerten oder neuem Verwendungszweck. Für den Einkauf bedeutet das: kein Go-live ohne Update-Governance.

Datenschutz- und Grundrechtssteuerung sind nicht nachgelagert, sondern Teil der Beschaffung.
Die DSK hält eine DSFA beim Einsatz von KI-Anwendungen vielfach für erforderlich und verlangt, dass Verantwortliche dafür schon bei Auswahl und Erwerb die nötigen Informationen vom Anbieter erhalten. Die BfDI geht noch einen Schritt weiter und empfiehlt ausdrücklich, DSFA als integralen Bestandteil der KI-Beschaffung und -Entwicklung zu organisieren; bei bestimmten Hochrisiko-Einsätzen öffentlicher Stellen ist ergänzend eine Grundrechte-Folgenabschätzung nach Artikel 27 durchzuführen.

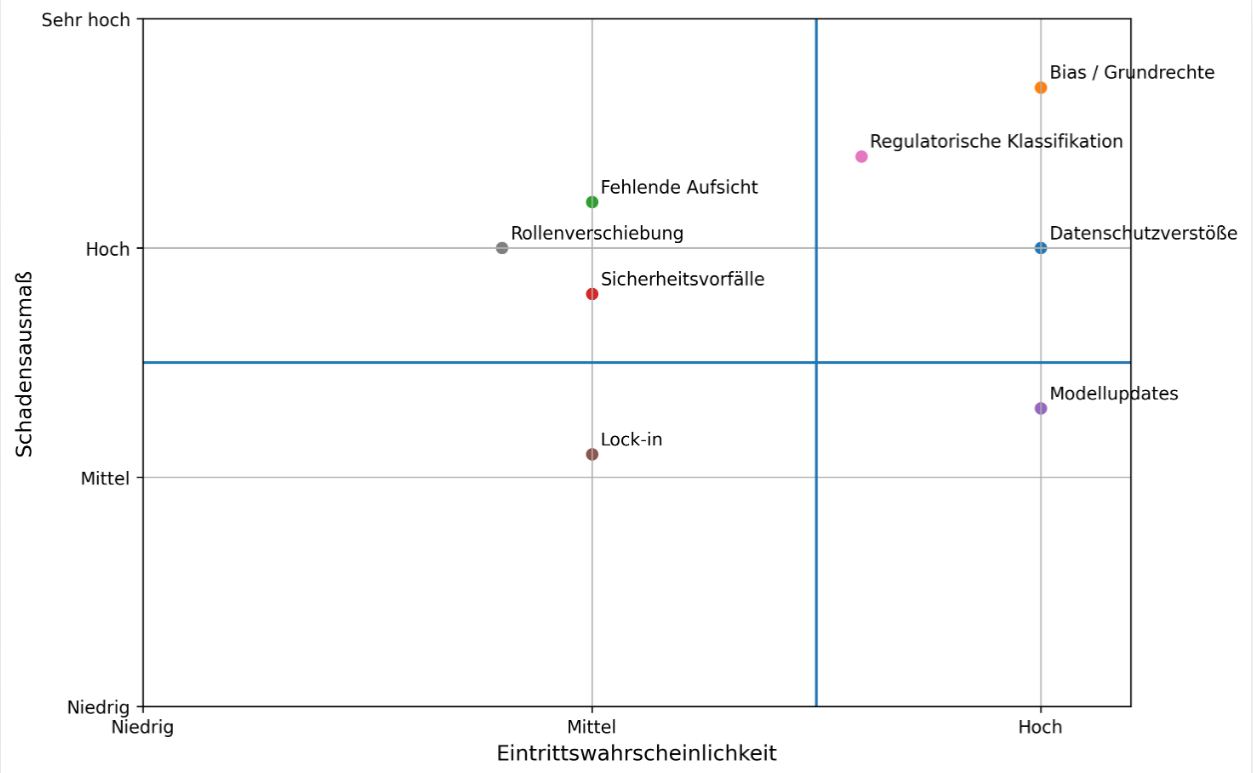
Mindestanforderungen an Beschaffung und Einsatz

Anforderung	In der Beschaffung klären	Im Betrieb sicherstellen	Nachweis
Klassifikation	KI-System oder IT? Risiko-Level klären	Freigabe durch Recht/Compliance	Use-Case-Sheet
Rollenklärung	Anbieter-und Betreiberrollen definieren	Keine ungewollte Provider-Rolle	Rollenmatrix
Dokumentation	Herstellerinfos, Modellbeschreibung	Vollständig und aktuell verfügbar	Dokumentationspaket
Datenschutz	Datenarten, Rechtsgrundlagen, Training	DSFA, Betroffeneninfos umgesetzt	TOMs, DSFA
Tests & Metriken	Leistungs- und Qualitätskriterien	Abnahmetests & Fehlerszenarien	Testprotokolle
Human Oversight	Menschliche Kontrolle definieren	Verantwortliche & Eskalation	RACI, Schulung
Logging & Monitoring	Relevante Events festlegen	Laufendes Monitoring & Alerts	Monitoring-Konzept

Updates	Update- und Änderungsrechte klären	Keine Änderungen ohne Freigabe	Release-Prozess
Incident Management	Meldewege definieren	Reaktion & Ursachenanalyse	Incident-Runbook
Exit & Lock-in	Datenexport & Wechseloptionen	Exit-Test vor Vertragsende	Exit-Plan
KI-Kompetenz	Schulungsbedarf definieren	Regelmäßige Qualifizierung	Schulungsnachweis

Die Tabelle verdichtet Mindestanforderungen aus Artikeln 4, 9–15, 18, 19, 20, 26, 49, 72 und 73 der KI-Verordnung, aus den Datenschutzleitlinien deutscher Aufsichtsbehörden sowie aus einschlägigen Standardisierungs- und Managementsystemansätzen. Für Governance und Nachweisführung sind insbesondere harmonisierte AI-Act-Standards in Vorbereitung; bis dahin sind ISO/IEC 42001, ISO/IEC 23894 und ISO/IEC 27001 als belastbare Strukturgeber nützlich, auch wenn sie die gesetzlichen Pflichten nicht ersetzen.

Risikobewertungsmatrix für die Beschaffung

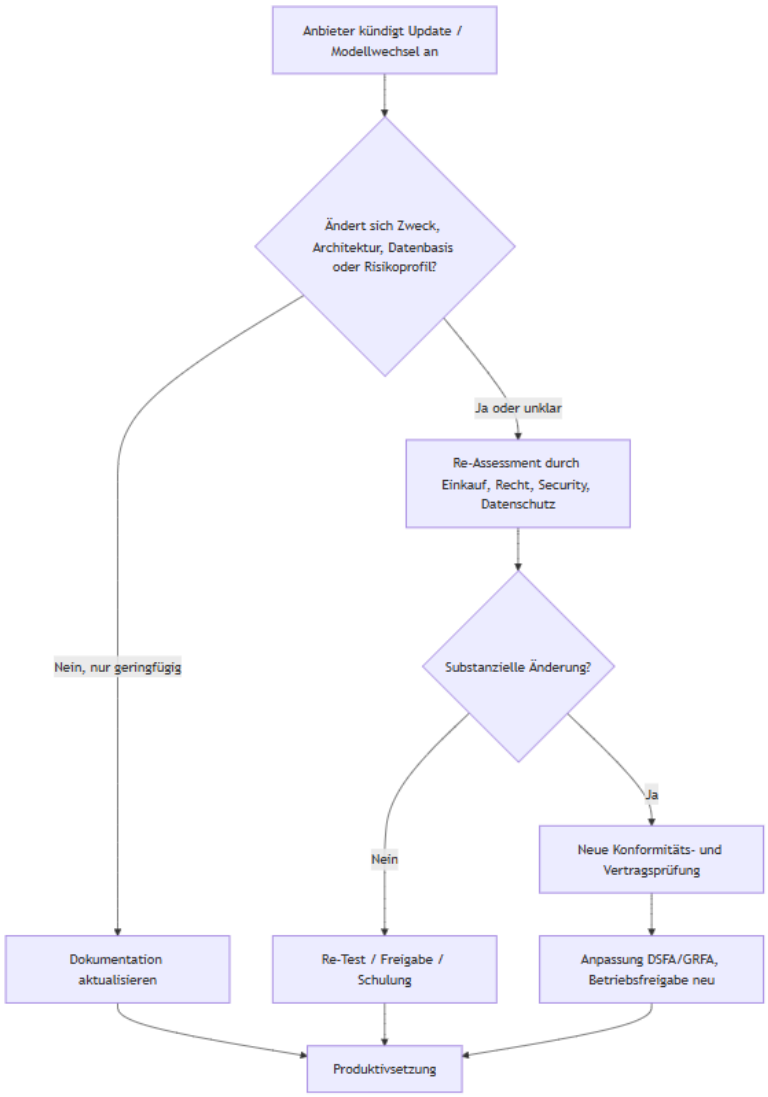


Die Matrix ist eine praxisorientierte Synthese aus dem risikobasierten AI-Act-Ansatz, der Datenschutzaufsicht und den ISO-Risikomanagementansätzen. Sie sollte im Unternehmen nicht generisch bleiben, sondern pro Use Case mit konkreten Schwellen, Verantwortlichkeiten und Residualrisiken befüllt werden.

Vergabe, Verträge und Anforderungsmanagement

Für öffentliche Auftraggeber ist KI selten ein Fall für die simpelste Verfahrenslogik. Die Vergaberichtlinie erlaubt ausdrücklich vorläufige Marktkonsultationen, Verhandlungsverfahren, wettbewerblichen Dialog und Innovationspartnerschaften. Zugleich stellt Artikel 67 klar, dass der Zuschlag auf das wirtschaftlich günstigste Angebot zu stützen ist und neben Preis oder Kosten auch qualitative, innovative, umwelt- oder soziale Kriterien einbeziehen darf; Artikel 68 erlaubt Lebenszykluskostenansätze. Für KI heißt das praktisch: Funktions- und Governanceanforderungen, Daten- und Sicherheitsarchitektur, Änderungsregeln und Betriebseignung sind regelmäßig wichtiger als ein isolierter Lizenzpreis.

Selbst in privatrechtlichen Beschaffungen sollte die Leistungsbeschreibung funktionsorientiert und evidenzbasiert gebaut werden. Gute KI-Anforderungsmanagement-Dokumente definieren deshalb nicht nur Features, sondern *zulässige Einsatzzwecke*, *unzulässige Entscheidungen*, *erforderliche Nachweise*, *Metriken*, *Verifikationsszenarien*, *personenbezogene Daten*, *Prompt- und Modellschnittstellen*, *Zulieferer/Subprozessoren* und *Exit-Pfade*. Besonders kritisch ist, dass die Dokumentation des Anbieters nicht bloß versprochen, sondern als Liefergegenstand, Mitwirkungspflicht und Aktualisierungspflicht ausgestaltet wird.



Dieser Ablauf folgt der Logik der substanziellen Änderung, der DSFA-/GRFA-Integration und des Post-Market-Monitorings.

Musterklauseln für KI-Verträge

Die folgenden Klauseln sind bewusst kurzgehalten und als Verhandlungsbausteine gedacht. Sie ersetzen keine Einzelfallprüfung, bilden aber die typischen Soll-Punkte eines belastbaren KI-Vertragsrahmens ab. Ihre Struktur orientiert sich an AI-Act-, Datenschutz- und Aufsichtsanforderungen.

Haftung und regulatorische Verantwortlichkeit

Der Anbieter sichert zu, dass das vertragsgegenständliche KI-System für den vereinbarten Verwendungszweck nach dem bei Vertragsschluss bekannten Rechtsrahmen konzipiert ist und er die ihm zugewiesenen regulatorischen Pflichten erfüllt. Entstehen dem Auftraggeber Schäden, Kosten oder behördliche Maßnahmen aufgrund einer vom Anbieter zu vertretende Pflichtverletzung, insbesondere wegen unzutreffender Angaben zur Klassifikation, fehlender Dokumentation, nicht gemeldeter Non-Compliance oder unzulässiger Datenverarbeitung, stellt der Anbieter den Auftraggeber im vereinbarten Umfang frei.

Audit, Dokumentation und Mitwirkung

*Der Anbieter stellt dem Auftraggeber und auf begründete Anforderung dessen Prüfer*innen sämtliche zur rechtlichen, technischen und sicherheitsbezogenen Bewertung erforderlichen Informationen, Nachweise und Dokumentationsstände rechtzeitig zur Verfügung. Der Auftraggeber ist berechtigt, risikobasiert Audits, Dokumentenprüfungen, Testbeobachtungen und Kontroll-gespräche durchzuführen oder durchführen zu lassen; Betriebs- und Geschäftsgeheimnisse sind angemessen zu schützen.*

Datenschutz und Training mit Eingaben/Ausgaben

Personenbezogene oder vertrauliche Eingaben, Ausgaben, Chats, Prompts, Protokolle oder abgeleitete Artefakte des Auftraggebers dürfen nicht für das Training, Retraining, Fine-Tuning oder die allgemeine Verbesserung von Modellen des Anbieters oder Dritter verwendet werden, soweit dies nicht im Einzelfall ausdrücklich und gesondert schriftlich freigegeben ist. Der Anbieter setzt hierzu technische und organisatorische Sperren um und weist diese auf Verlangen nach.

Modellupdates und Change Control

Kein Wechsel des Basismodells, der Modellversion, der Datenquellen, der wesentlichen Parameter, der Prompt-Orchestrierung oder der Sicherheitsarchitektur darf produktiv wirksam werden, bevor der Anbieter den Auftraggeber vorab informiert, die Änderung klassifiziert und dem Auftraggeber die für eine Re-Bewertung erforderlichen Informationen bereitgestellt hat. Der Auftraggeber kann bei rechtlichem, fachlichem oder sicherheitsbezogenem Risiko die Produktivsetzung aussetzen.

Monitoring, Logging und Incident Response

Der Anbieter betreibt ein angemessenes Monitoring für Leistung, Fehlerraten, Drift, Sicherheitsvorfälle und sonstige Abweichungen und informiert den Auftraggeber unverzüglich über relevante Incidents, plausible Verdachtsfälle und Corrective Actions. Er stellt die zur Ursachen-analyse, Nachweisführung und Aufsichtskommunikation erforderlichen Logs, Reports und

*Ansprechpartner*innen zur Verfügung.*

Praktische Checkliste vor Go-live

- Vertragsanhänge mit Rollenmatrix, Dokumentationsliste, TOMs und Update-Prozess sind final.
- Test- und Abnahmekriterien wurden mit echten Fachszenarien geprüft.
- DSFA ist abgeschlossen; GRFA wurde – soweit erforderlich – koordiniert.
- Human-Oversight-Rollen, Eskalationswege und Override-Rechte sind benannt.
- Schulungen/KI-Kompetenzmaßnahmen sind durchgeführt und dokumentiert.
- Produktiv- und Supportmodell, Logs, Incident-Prozess und Ausstiegsoption sind freigegeben.
- Betriebs- oder Personalvertretung wurde – soweit erforderlich – eingebunden.
- Kommunikationspflichten gegenüber Betroffenen, Beschäftigten oder Kund*innen sind vorbereitet.

Diese Go-live-Checkliste folgt den Vorgaben zur Transparenz, Aufsicht, DSFA/GRFA, KI-Kompetenz und Dokumentations-/Monitoringpflicht.

Praxisbeispiele

Das Register der Stadt Amsterdam zeigt, wie Transparenz- und Impact-Governance auch nach der Beschaffung organisatorisch verankert werden können. In den veröffentlichten Einträgen werden Status, Einsatzbereich und teils konkrete Impact- oder Datenschutzprüfungen wie DPIA/Privacy Quickscan angegeben. Für die Beschaffungspraxis ist der Kernpunkt nicht das Register selbst, sondern die Voraussetzung dafür: Der Lieferant oder interne Entwickler muss die nötigen Metadaten, Test- und Wirkungsunterlagen überhaupt liefern können.

Die Stadt Helsinki betreibt ein öffentliches AI-Register als „Fenster“ in die dort eingesetzten KI-Systeme. Der Governance-Mehrwert liegt in transparenter Use-Case-Dokumentation, einer Feedback-Möglichkeit und der Idee, KI nicht als Black Box, sondern als überprüfbaren Verwaltungsbaustein zu behandeln. Beschaffungsseitig spricht das für Pflichten zur laufenden Dokumentationspflege, nicht bloß für eine Dokumentenlieferung bei Vertragsbeginn.

Das Reallabor-Pilotprojekt in Deutschland ist für Beschaffer*innen besonders instruktiv. Laut Pressebericht der Bundesnetzagentur wurden dort seit 2025 anhand zweier Start-up-Anwendungsfälle Anforderungen, Abläufe und Herausforderungen von KI-Reallaboren simuliert; ein Ergebnis war eine detaillierte Roadmap für Medizinprodukte mit integriertem Hochrisiko-KI-System. Hervorgehoben werden insbesondere behördenübergreifende Zusammenarbeit, Reifegradmodelle, Vertraulichkeit, schriftliche Nachweise und die Beschleunigung späterer Konformitätsbewertung. Für innovative KI-Beschaffung ist das ein starkes Argument für phasenweise Verträge statt Big-Bang-Einkauf.

Der Fall der italienischen Datenschutzaufsicht Garante per la protezione dei dati personali gegenüber OpenAI zeigt die Gegenprobe. 2023 beanstandete die Behörde insbesondere fehlende Informationen, eine fehlende Rechtsgrundlage für die massenhafte Datenverarbeitung zu Trainingszwecken, Datenungenauigkeit und fehlende Altersverifikation. Nach zusätzlichen Transparenz-, Opt-out- und Altersmaßnahmen wurde der Zugang in Italien wieder geöffnet. Für Beschaffer*innen lautet die Lehre: Datenschutz und Trainingsregeln sind nicht „Nebenkriegsschauplätze“, sondern echte Beschaffungs- und Betriebsrisiken mit unmittelbarer Marktwirkung.

Umsetzungsfahrplan und Vorlagen

Wer heute ein belastbares KI-Beschaffungsmodell aufsetzen will, braucht kein mehrjähriges Transformationsprogramm, sondern einen konsequenten Zwölfmonatsfahrplan mit frühen Mindeststandards und späterer Verfeinerung. Die folgenden Phasen sind als einseitig darstellbare Roadmap für Word geeignet. Sie spiegeln die offiziellen Prioritäten zu KI-Kompetenz, Service-Desk-/Kompass-Unterstützung, Reallaboren, Standardisierung und risikobasiertem Roll-out wider.

Roadmap und Zeitachs

Phase	*Fokus*	*Ergebnis*
Monat 1	Transparenz schaffen	KI-Portfolio
Monat 2–3	Mindeststandards	Beschaffungsstandard v1
Monat 3–4	Governance	Governance v1
Monat 4–6	Verträge & Pilotierung	Kontrollset
Monat 6–9	Integration	Regelbetrieb v2
Monat 9–12	Optimierung	Reifegradbericht

Empfohlene Vorlagen

Interne Vorlagen, die jede Organisation sofort anlegen sollte

- KI-Use-Case-Sheet mit Klassifikation, Datenarten, Zweck, Betroffenenkreis, Autonomiegrad
- Anbieter-Due-Diligence-Fragebogen mit Fokus auf Dokumentation, Training, Updates, Subunternehmer, Logs, Incident-Prozess
- DSFA-/GRFA-Kopplungsblatt für öffentliche Stellen und regulierte Kontexte
- Test- und Abnahmekatalog für fachliche, technische, Bias-, Security- und Fallback-Szenarien
- Update-/Modellwechsel-Formular mit Substantial-Modification-Prüfung
- Incident- und Corrective-Action-Protokoll
- Exit- und Migrationsplan
- KI-Kompetenzmatrix nach Rollen

Offizielle oder quasi-offizielle Werkzeuge, die man sofort nutzen sollte

- KI-Service-Desk und KI-Compliance-Kompass der Bundesnetzagentur als erste Einordnungshilfe für Risiko, Pflichten und deutsche Umsetzungslogik.
- AI Act Service Desk und FAQ des europäischen KI-Ökosystems für Artikel- und Rollenauslegung, insbesondere zu Hochrisiko, GPAI, Transparenz und Timeline.

- AI-Literacy-Q&A und Praxisrepository des europäischen KI-Büros für Aufbau und Dokumentation von KI-Kompetenz.
- DSK-Orientierungshilfe und BfDI-Handreichung als belastbare Datenschutz- und Governance-Referenzen, insbesondere für DSFA, Beschäftigtenkontext, Monitoring und vertraglichen Ausschluss des Trainings mit Eingaben/Ausgaben.
- ProcurCompEU für Kompetenzprofile in der öffentlichen Beschaffung.
- ISO/IEC 42001, 23894 und 27001 als Strukturgeber für AIMS, KI-Risikomanagement und Informationssicherheit.

Kernaussage für die Praxis

Die tragfähige Beschaffungsstrategie für KI ist weder „möglichst früh einkaufen“ noch „erst alles regulatorisch abwarten“. Richtig ist ein dritter Weg: standardisieren, klassifizieren, dokumentieren, phasenweise beauftragen, Updates kontrollieren und den Betrieb aktiv überwachen. Genau dort liegt die Balance zwischen Innovation und Haftung.

Passende Weiterbildungen finden Sie hier:

Weiterbildung zum Thema Recht

Finden Sie aus unserem erstklassigen Weiterbildungsangebot die für Ihre Bedürfnisse passende Fortbildung. Profitieren Sie von unseren maßgeschneiderten Seminaren und Lehrgängen mit erfahrenen, hochkarätigen Experten rund um das Thema Recht. Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

Wir garantieren fachlich hochwertige Weiterbildung für Ihren Erfolg – unsere ISO-Zertifizierungen nach 9001 und 21001 unterstreichen dies. Jetzt informieren

FORUM · Institut für Management GmbH · Postfach 10 50 60 · 69040 Heidelberg · Germany
Telefon: +49 6221 500-500 · Fax: +49 6221 500-555 · www.forum-institut.de